Additional Help: 545
File Name: 545saf_062501_cd24
Last Revised: 06/21/2001

Synopsis of Security Rules of Behavior for Users

This brief synopsis of security **rules of behavior** for users of unclassified information systems (IS) is provided to assist in understanding the guidance provided in ADS 545. This document is not all-inclusive; for additional assistance on security matters relating to processing unclassified data, contact your Information System Security Officer (ISSO.)

1. Read, understand, and implement/execute:

    a. IS security policies.

    {Automated Directives System (ADS), State Department Guidance etc.}

    b. IS security forms.

    {Authorized Access List, Fax Cover Sheet, USAID Computer System Access & Termination Request, USAID Sensitive Data Nondisclosure Agreement, USAID Unclassified Information Systems Access Request Acknowledgement, Visitor's Log etc.}

2. Make your password(s) unique and hard to guess or "crack."

3. Use current anti-virus software to scan data (especially new data).

4. Log off your workstation when you leave your area.

5. Back up your files.

6. Follow the Agency's rules of behavior. Some user rules of behavior are

    a. Access only data you are authorized to use:

        (1) Don't use or change any account, file, record, or application (software program) not required to perform your official duties or officially authorized activities.

        (2) Don't access someone else's account or files without formal authorization from your supervisor.

        (3) Remember not to access or disclose sensitive or personal data unless it is necessary to perform your official duties.

b. Work with others to administer necessary safeguards and controls:

(1) Cooperate with inspectors and evaluators.

(2) Assist in the completion of the information system certification and accreditation/approval to operate process, and contingency planning for information resources.

(3) Participate in IS security training and awareness programs.

c. Be careful with IS resources (software, hardware, communications means, etc.):

(1) Don't move equipment or exchange components without authorization from the appropriate Information Technology (IT) Systems support element.

(2) Protect IS resources from physical hazards such as liquids, food, smoke, staples, paper clips, etc.

(3) Don't install or use unauthorized software on IS.

(4) Comply with all software licensing agreements; don't violate Federal copyright laws.

(5) Don't overload systems with extraneous matter (e.g., keep e-mail attachments small, avoid excessive graphics on web pages, limit length of facsimile transmissions etc).

7. Report IS security incidents (see diagram **below**).

User Identifies System Anomaly, Then Assesses -- Is It:

A technical glitch? **or** **due to wrongful action (virus, etc.)?**

Contact System Admin, Site ISSO. - In USAID/W Call Help Desk at 202-712-1234

Contact Site ISSO, Program Manager; Site ISSO will contact either USAID ISSO at 202-712-4559 or FRAIM 9 ISS Team Program Manager at 703-465-7054 or Information Assurance Data (IAD) Fusion Center at 202-712-0347, e-mail CAssistance@usaid.gov

NOTE: Write down when (date/time) the anomaly occurred; summarize details: application/software affected, impact on USAID activities etc.